



McAfee
Together is power.

Securing Tomorrow. (https://securingtomorrow.mcafee.com/)
Today.



```
(var b = [], c = 0; c < a.length; c++) { 0 == use_array(a[c], b) && b.push(a[c]); } return b.length;
function count_array_gen() { var a = 0, b = $("#User_logged").val(), b = b.replace(/(\r\n|\n|\r)/gm, " "), b
laceAll(" ", " ", b), b = b.replace(/+(?= )/g, ""); inp_array = b.split(" "); input_sum = inp_array.le
for (var b = [], a = [], c = [], a = 0; a < inp_array.length; a++) { 0 == use_array(inp_array[a], c) && (
p_array[a]), b.push({word:inp_array[a], use_class:0}), b[b.length - 1].use_class = use_array(b[b.length - 1
np_array)); } a = b; input_words = a.length; a.sort(dynamicSort("use_class")); a.reverse(); b =
exOf_keyword(a, " "); -1 < b && a.splice(b, 1); b = indexOf_keyword(a, void 0); -1 < b && a.splice(b,
p = indexOf_keyword(a, ""); -1 < b && a.splice(b, 1); return a; } function replaceAll(a, b, c) { retu
ce(new RegExp(a, "g"), b); } function use_array(a, b) { for (var c = 0, d = 0; d < b.length; d++) { b[
c++; } return c; } function czy_juz_array(a, b) { for (var c = 0, c = 0; c < b.length && b[c].word !
{ } return 0; } function indexOf_keyword(a, b) { for (var c = -1, d = 0; d < a.length; d++) { if (
l == b) { c = d; break; } } return c; } function dynamicSort(a) { var b = 1; "-." ==
(b = -1, a = a.substr(1)); return function(c, d) { return(c[a] < d[a] ? -1 : c[a] > d[a] ? 1 : 0) *
function occurrences(a, b, c) { a += " "; b += " "; if (0 >= b.length) { return a.length + 1; }
```

in f t G+ s

Malware Mines, Steals Cryptocurrencies From Victims

By **Tim Hux** (https://securingtomorrow.mcafee.com/author/tim-hux/) and **Norris Brazier**
(https://securingtomorrow.mcafee.com/author/norris-brazier/) on **Nov 22, 2017**
(https://securingtomorrow.mcafee.com/2017/11/)

How's your Bitcoin balance? Interested in earning more? The value of cybercurrency is going up. One way to increase your holdings is by "mining," (https://www.bitcoinmining.com/) which is legal as long as it is done with the proper permissions. Using your own mining equipment or establishing a formal agreement for outsourcing are two methods. Hardware vendors such as Asus manufacture motherboards that are specifically tailored for mining cryptocurrency.

Bitcoin mining involves complex mathematical calculations that are carried out by a computer's hardware and result in transaction records. These records are added to the Bitcoin public ledger, the "blockchain." The ledger keeps track of all transactions and verifies these transactions are legitimate.

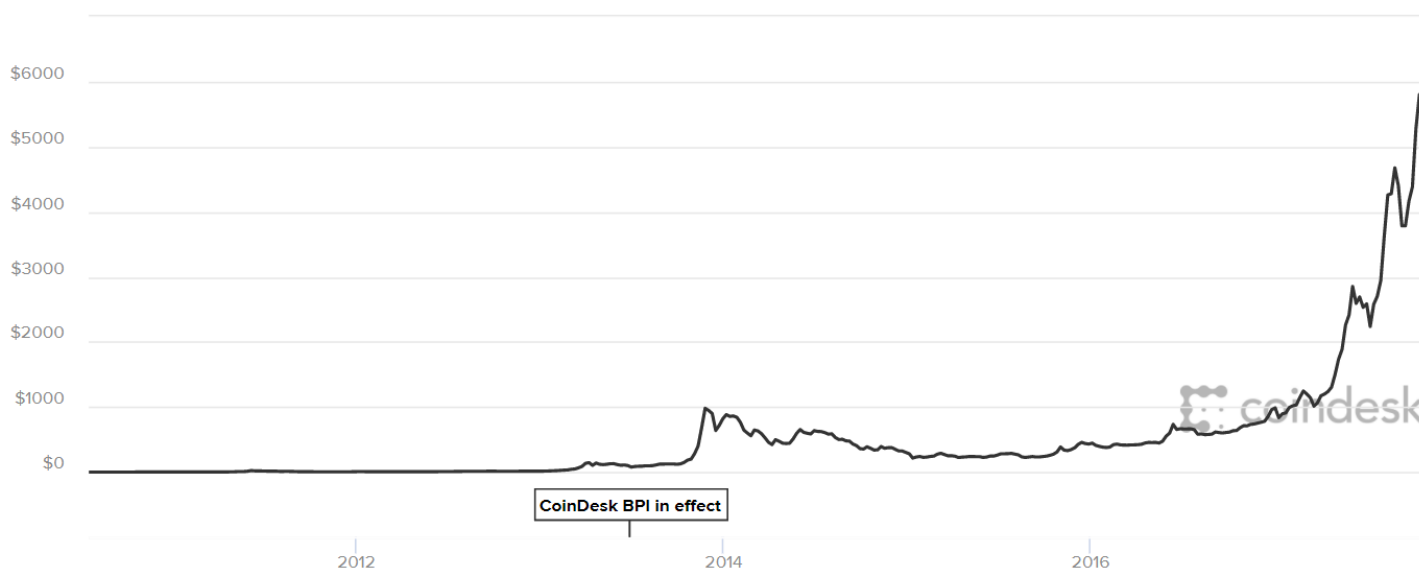
Cybercriminals are also attracted to online currency, which fuels much of their business, including malware purchases and ransomware payments. Cybercriminals would rather find outside computing power instead of using their own equipment because the price of a dedicated mining machine could exceed US\$5,000. Cybercriminals often seek to bypass the agreement phase and maliciously introduce malware that will either use a victim's computing power to mine for coins or simply locate and steal the user's cryptocurrency.

AntMiner S7**AntMiner S9****Avalon6**

Three popular Bitcoin miners (<https://www.bitcoinmining.com/bitcoin-mining-hardware/>).

The number of instances of mining malware has increased significantly, to 1.65 million victims this year, according to one report. (<https://securelist.com/miners-on-the-rise/81706/>) That's a lot of slowing machines and increased electricity costs. For individual users, the slowness and increased electricity bill may be trivial, and go unnoticed for a time. For businesses with hundreds or thousands of machines, however, the cost increase can be substantial.

The increased interest in illegally mining or stealing cryptocurrencies correlates easily with the increased value of these currencies. One Bitcoin (BTC) was recently worth more than \$7,500, up from around \$3,000 a few weeks ago. Even considering an earlier decline in value, Bitcoin has been trending upward for years. This upswing in value and the recent adoption of Bitcoin in Japan and South Korea as a legal tender (<https://cointelegraph.com/news/japan-officially-recognizes-bitcoin-and-digital-currencies-as-money>) have increased the demand for acquiring Bitcoin and altcoins. In September cybercriminals stole \$63,000 (<https://blog.eset.ie/2017/09/28/money-making-machine-monero-mining-malware/>) worth of cryptocurrency in about three months by taking advantage (<https://thehackernews.com/2017/09/windows-monero-miners.html>) of a flaw in Microsoft Windows Internet Information Services.



The price of Bitcoin since 2010. Source: CoinDesk. (<https://www.coindesk.com/price/>)

Initial coin offerings (https://en.wikipedia.org/wiki/Initial_coin_offering)(ICOs) have also contributed to this gold rush. ICOs are similar to IPOs but instead of issuing to investors shares of a new company, the investors are given cryptocurrency in the hopes a new company will be successful and result in a higher value for their digital coins.

During the last few years we have seen an increase in innovation by malware authors to infiltrate this space, resulting in malware that both mines or steals coins and spans various and platforms. Let's break down some of the tools and techniques in the world of crypto-mining/-stealing malware that has arisen.

- NightMiner
- Adylkuzz
- EternalMiner
- MulDrop.14
- ELF Linux/Mirai
- OSX/Miner-D
- Dridex
- Trickbot
- Jimmy Nukebot
- HawkEye
- Cerber
- Web Mining

NightMiner

NightMiner mining malware was first seen in the wild in March 2015 and has been used to mine the Monero cryptocurrency. Some cybercriminals have turned to Monero due to its built-in security features and lower cost to mine. For example, Monero by default supports many blockchain (<https://securingtomorrow.mcafee.com/mcafee-labs/staying-anonymous-on-the-blockchain-concerns-and-techniques/>) obfuscation and anonymity technologies such as stealth addresses and crypto notes. This malicious software has been discovered on network attached storage (NAS) devices and takes advantage of those devices' powerful CPU and GPU resources. The mining software can stay under the radar on these devices because most administrators fail to install antimalware software on NAS systems. Sophos released an extensive report (<https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Cryptomining-malware-on-NAS-servers.pdf>) discussing this malware.

Adylkuzz

Adylkuzz (<https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar>) is more recent, coming on the scene in this year. The mining malware is similar to the well-known ransomware WannaCry in that it exploits two flaws in Microsoft's server message block (SMB) that are known as EternalBlue and DoublePulsar. Both defects were leaked by the Shadow Brokers hacking group and are believed to be the work of the U.S. National Security Agency's Equation Group. Adylkuzz is unique in that it will block all access to TCP Port 445, preventing other malware from taking advantage of the SMB flaws.

```
fb > USE Eternalblue
```

```
[!] Entering Plugin Context :: Eternalblue  
[*] Applying Global Variables  
[+] Set NetworkTimeout => 60  
[+] Set TargetIp => 192.168.206.147
```

Code snippet from the EternalBlue Metasploit module.

EternalMiner

Linux systems are not immune. EternalMiner (<https://www.bleepingcomputer.com/news/security/linux-servers-hijacked-to-mine-cryptocurrency-via-sambacry-vulnerability/>) took advantage of a vulnerability in Samba to infect as many systems as possible. The flaw allowed Samba servers to load and execute code remotely after a shared library was uploaded by a

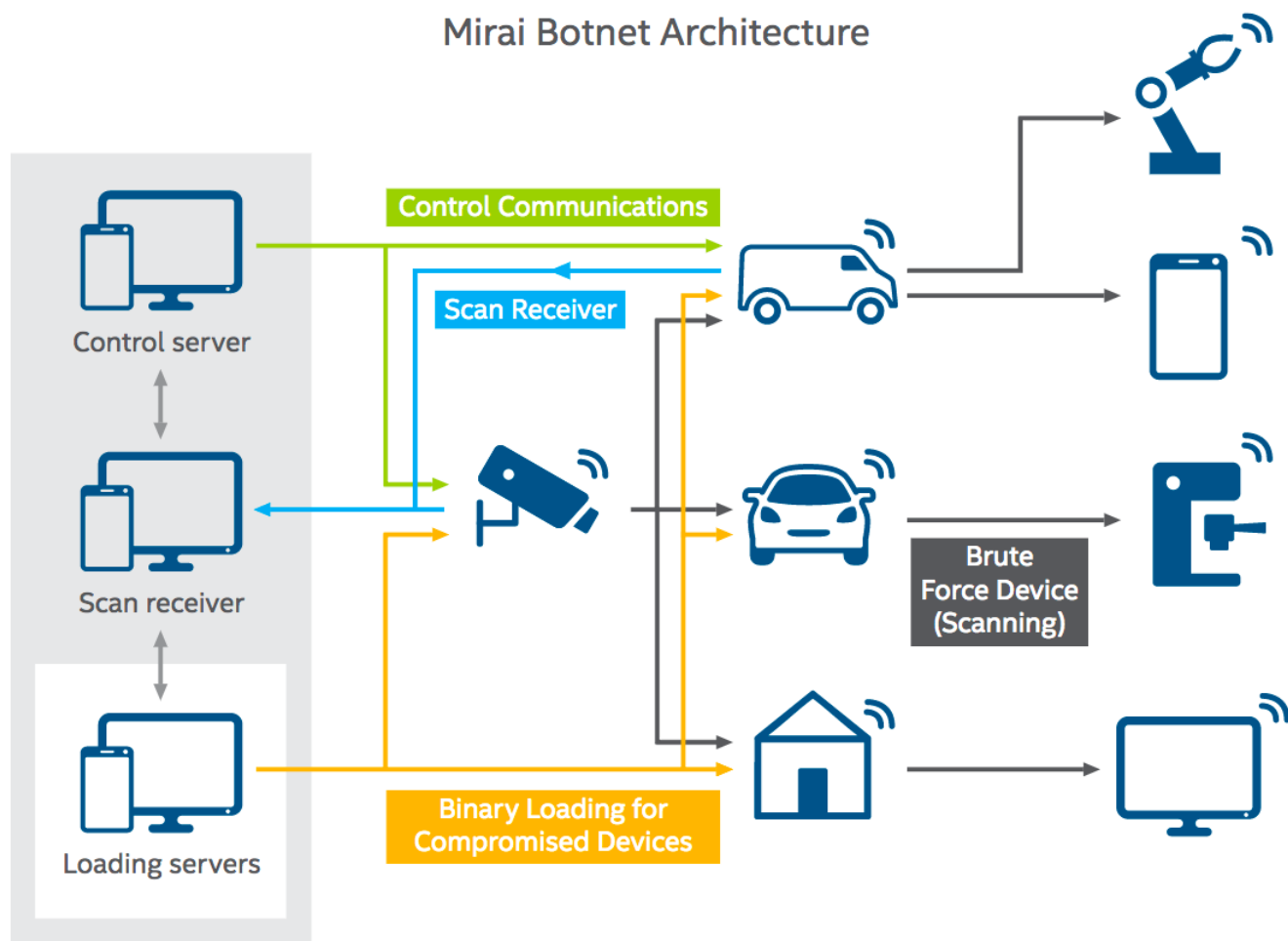
malicious client. A patch to address the seven-year-old flaw was released in May, but cybercriminals made thousands of dollars before network administrators could update their servers.

Linux.MulDrop.14

Researchers have seen instances of Raspberry Pi—a small, versatile single-board computer— attacked by the crypto mining malware Linux.MulDrop.14. (<http://www.zdnet.com/article/linux-malware-enslaves-raspberry-pi-to-mine-cryptocurrency/>) The malicious software does not attempt to mine the CPU-intensive Bitcoin but, like NightMiner, focuses on Monero. This action shows a level of innovation as cybercriminals expand their scope to acquire cryptocurrencies across additional platforms.

ELF Linux/Mirai

Cryptocurrency malware mining has been discovered in connection with the Mirai botnet. ELF Linux/Mirai continues to evolve and has added a Bitcoin miner slave module, allowing the malware to mine cryptocurrency from thousands of infected IoT devices, according to a report (<https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/>) from IBM X-Force. Mirai, ([https://en.wikipedia.org/wiki/Mirai_\(malware\)](https://en.wikipedia.org/wiki/Mirai_(malware))) discovered in August 2016, infected IoT devices and has also been responsible for several DDoS attacks, including against DNS provider Dyn and Liberia's Internet infrastructure.



Source: McAfee Labs Threats Report, March 2017 (<https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf>)

OSX/Miner-D

Although Apple's Mac OS has not been heavily targeted, it is also not immune. OSX/Miner-D both steals Bitcoins and mines a system. This malware has been around since 2011 and is the second most common malware (<https://www.bleepingcomputer.com/news/security/the-second-most-popular-mac-malware-is-a-cryptocurrency-miner/>) on the Mac. The malware, which is inserted into legitimate apps uploaded to torrent sites, made a surge early this year and resulted in more than 20% of all detections in May. We expect to soon see new variants of this malicious software.

Dridex

Cryptocurrency mining has caught the attention of the Dridex (<https://blogs.forcepoint.com/security-labs/dridex-shadows-blacklisting-stealth-and-crypto-currency>) Trojan's developers. Dridex is a banking Trojan that steals credentials to access accounts. Samples of this malware were discovered in 2016 that find and steal cryptocurrency wallets.

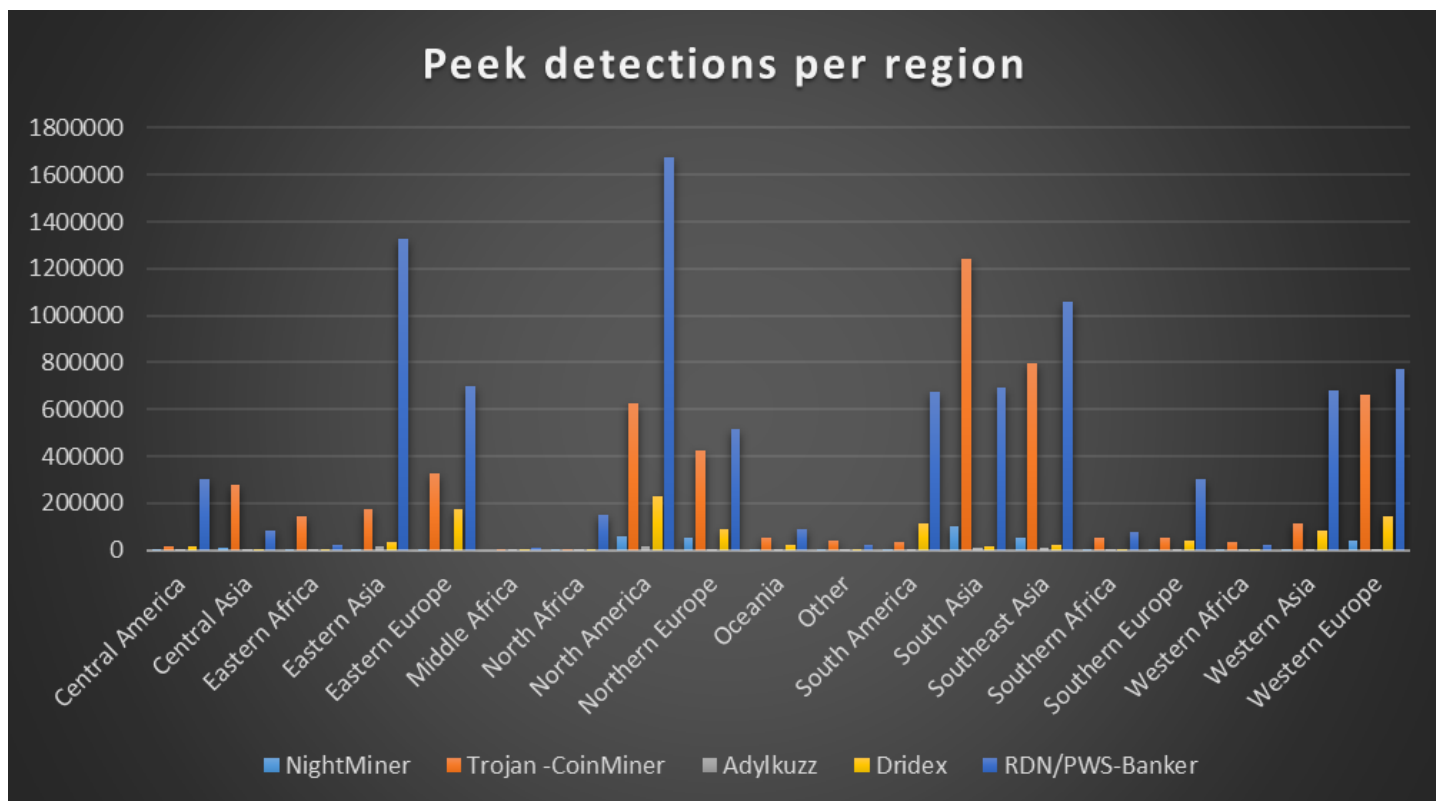
Dridex is sophisticated malware. The developers behind this malware continue to evolve its code to avoid detection, increase infections, distribute ransomware, steal banking and personal information, and now pilfer Bitcoins.

Trickbot

The cybercriminals behind Trickbot (<https://blogs.forcepoint.com/security-labs/trickbot-goes-after-cryptocurrency>) have added the capability to steal cryptocurrency. Trickbot has been around for years and has recently added [coinbase.com](https://www.coinbase.com/) as one of its attack vectors. Once a system is infected, the malware monitors the victim's browsing habits and injects a fake login page whenever the user visits [coinbase.com](https://www.coinbase.com/). The fake page allows criminals to steal the login information, resulting in the theft of cryptocurrencies including Bitcoin, Ethereum, and Litecoin as well as other digital assets.

Jimmy Nukebot

Another Trojan making headlines is Jimmy Nukebot. (<https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/>) The authors behind the malicious software used code from the NeutrinoPOS banker Trojan. This variant, detected by McAfee as RDN/PWS-Banker, does not steal bank card data as before but installs various modules that contain a payload. One payload mines Monero. The digital wallet associated with the miner has received only about \$45, which may indicate the malware authors either changed wallets or have stopped mining, according to Kaspersky.



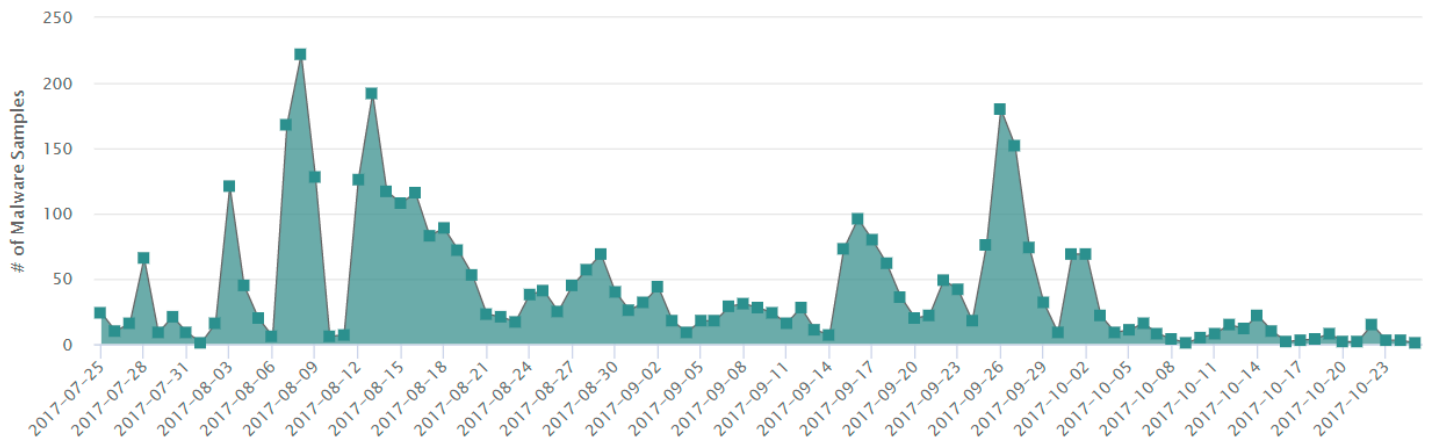
McAfee Labs detections for some variants of mining malware. Peek detections are the highest number of detection occurrences on a single date in 2017.

HawkEye

The credential harvesting malware HawkEye, (<https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html>) which surfaced in 2014, has added Bitcoin wallet stealing to its arsenal. The malware is well known for stealing a variety of credentials from web browsers and mail clients. Recent samples show HawkEye targeting the file wallet.dat, which holds the user's Bitcoin private keys along with other transaction information.

Cerber

Developers behind most ransomware prefer the ransoms be paid using cryptocurrency. In the recent case of Cerber, (<https://securingtomorrow.mcafee.com/business/cerber-ransomware-now-capable-stealing-browser-passwords-bitcoin-wallet-data/>) however, the actors have resorted to stealing the coins from the wallet before encrypting the system. Cerber is one of the most prolific ransomware families, infecting millions of computers worldwide. The ransomware has seen a decline in the past few months but continues to wreak havoc.



The number of Cerber samples detected during the last 90 days. Source: Ransomware Tracker.
(<https://ransomwaretracker.abuse.ch/>)

Web Mining

One new trend is a technique that mines cryptocurrency when visitors connect to websites.

(<https://www.bleepingcomputer.com/news/security/a-new-player-joins-coinhive-on-the-browser-cryptojacking-scene/>)

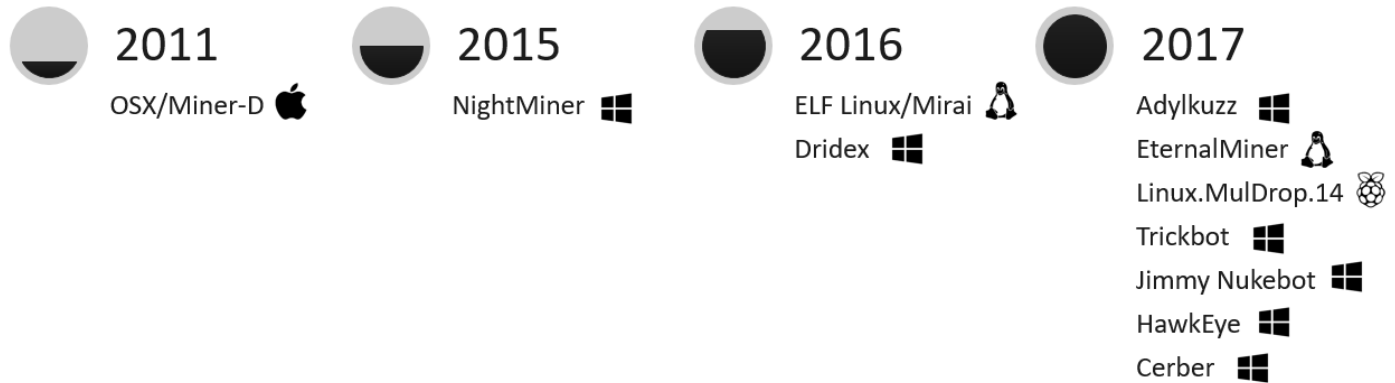
Coinhive and Crypto-Loot, as well as others, sell Monero mining software that allows the buyer to insert JavaScript into websites. The JavaScript mines cryptocurrency by using the site visitor's CPU power. The service has been a hot topic since it first appeared because the software can be used maliciously to allow cybercriminals to mine cryptocurrency without users consent. A few legitimate sites, including The Pirate Bay and a major television company, have recently been found using the software to mine Monero. The entertainment conglomerate has removed the code but it remains unclear whether hackers injected the software or if the company included the code to make a few extra dollars while unsuspecting users were watching their favorite shows.

The Pirate Bay has also removed the mining code and released a statement claiming the 24-hour test was designed to see if the popular file-sharing site could use the miner to generate revenue and potentially replace ads. A few other sites, including Iridium and PublicHD, are using the JavaScript code openly: Both sites inform their users of the code and in the case of Iridium allow them to opt out. The unsuspected use of web miners has caused some websites to go dark. Internet provider Cloudflare began shutting down (<https://www.coindesk.com/cloudflare-suspends-website-using-cryptocurrency-miner-malware/>) domains after the company discovered Coinhive's software mining Monero from visitors to torrent site ProxyBunker. The domains, which were shuttered for not allowing users to opt out, were reopened after removing the mining code.

```
options: {
  miner: {
    id: "miner",
    section: "donate",
    sub_section: "miner",
    type: "checkbox",
    value: false,
    i18n: {
      label: "Contribute using your computer"
    }
  },
  miner_threads: {
    id: "miner_threads",
    section: "donate",
    sub_section: "miner",
    type: "custom",
    value: window.navigator.hardwareConcurrency ? Math.round(window.navigator.hardwareConcurrency / 2) : 1,
    i18n: {
      thread_number: "Threads: "
    }
  }
}
```

JavaScript code from Iridium's Google Chrome miner extension.

Crypto mining is not new, but it has gained attention due to the popularity of cryptocurrency, ICOs, and the overall value increase of alt coins. As the adoption rate for cryptocurrency grows, we can expect cybercriminals to increasingly illegally mine or steal cryptocurrency. They can exploit online funds to shop on the dark web or in exchange for real currency.



A timeline of leading cryptocurrency miners.

< Previous Article (<https://securingtomorrow.mcafee.com/consumer/family-safety/dont-let-the-grinch-hack-your-christmas/>)

Next Article > (<https://securingtomorrow.mcafee.com/business/innovating-adversary-part-2/>)

📁 Categories: McAfee Labs (<https://securingtomorrow.mcafee.com/category/mcafee-labs/>)

🏷️ Tags: computer security (<https://securingtomorrow.mcafee.com/tag/computer-security/>), cybercrime (<https://securingtomorrow.mcafee.com/tag/cybercrime/>), cybersecurity (<https://securingtomorrow.mcafee.com/tag/cybersecurity/>), endpoint protection (<https://securingtomorrow.mcafee.com/tag/endpoint-protection/>), malware (<https://securingtomorrow.mcafee.com/tag/malware/>)

Leave a reply

[Facebook Comments \(1\)](#) [Comments \(0\)](#) [G+ Comments](#)

1 Comment

Sort by **Newest**

Add a comment...

**Praveen Gaikwad** · Manager at Tata Communications

Does McAfee End Point Products like VSE 8.8 detects and prevents Crypto Jacking attacks.

Like · Reply · 5w

**McAfee**

Hi Praveen,

If the attack uses a binary we classify as unsafe, our products will stop it. To be more clear, if we've seen it before (or we haven't, but it breaks our rules), we stop it. Beyond that, I'd need some additional details to give you a better answer (for example, your product configuration might have been changed for something else in your environment, changing how our product deals with certain threats). If we can answer more questions for you, or you'd like to try a free trial, check out <https://www.mcafee.com/us/products.aspx>.

Thanks!

Like · Reply · 2w

[Facebook Comments Plugin](#)

Newsletter Sign Up

First Name *

Last Name *

Email Address *

Country *

--Please Select--



Submit

McAfee on Twitter

 Follow us on Twitter (<https://twitter.com/McAfee>)[mcafee_labs \(https://www.twitter.com/mcafee_labs\)](https://www.twitter.com/mcafee_labs)

RT @ChristiaanBeek (<https://twitter.com/ChristiaanBeek>): 3D-printing someone's pelvis. @McAfee's Advanced Threat Research team finds vulnerabilities and best-practices failures...

[3 hours ago \(2018/03/12 05:06:04\)](#)

Reply (https://twitter.com/intent/tweet?in_reply_to=973062547266985987) · Retweet (https://twitter.com/intent/retweet?tweet_id=973062547266985987) · Favorite (https://twitter.com/intent/favorite?tweet_id=973062547266985987)



mcafee_labs (https://www.twitter.com/mcafee_labs)

RT @McAfee (<https://twitter.com/McAfee>): "The results were disturbing; ultimately, we were able to combine attack vectors to reconstruct body parts from the images and..."

[3 hours ago \(2018/03/12 04:51:23\)](#)

Reply (https://twitter.com/intent/tweet?in_reply_to=973058851040763905) · Retweet (https://twitter.com/intent/retweet?tweet_id=973058851040763905) · Favorite (https://twitter.com/intent/favorite?tweet_id=973058851040763905)



mcafee_labs (https://www.twitter.com/mcafee_labs)

RT @VentureBeat (<https://twitter.com/VentureBeat>): McAfee reports surge in healthcare, fileless malware, and cryptocurrency mining attacks <https://t.co/cd9A2B1SmD> (<https://t.co/cd9A2B1SmD>) by @deantak

[4 hours ago \(2018/03/12 04:27:45\)](#)

Reply (https://twitter.com/intent/tweet?in_reply_to=973052904440348672) · Retweet (https://twitter.com/intent/retweet?tweet_id=973052904440348672) · Favorite (https://twitter.com/intent/favorite?tweet_id=973052904440348672)

Next Article

(<https://securingtomorrow.mcafee.com/business/innovating-adversary-part-2/>)



Business (<https://securingtomorrow.mcafee.com/category/business/>)

Out Innovating the Adversary, Part 2

About (<https://www.mcafee.com/us/about-us.aspx>) | Subscribe ([/feed/](https://www.mcafee.com/us/about-us.aspx#feed/))

| Contact & Media Requests (<https://www.mcafee.com/us/about/contact-us.aspx#ht=tab-publicrelations>)

| Privacy Policy (<https://www.mcafee.com/common/privacy/english/index.htm>) | Legal (<https://www.mcafee.com/us/about/legal/legal-notices.aspx>)

© 2018 McAfee LLC



(https://~~https://~~~~https://~~~~https://~~~~https://~~~~https://~~)